Fri Mar 4 18:37:10 EST 1988

DSB Task Force On START Verification

Paradox: Counting versus concealment of mobile systems in a cooperative framework.

Since concealment in real time is the raison-d'etre of mobility we have a familiar paradox. How can we expect cooperation that would permit concealed systems be counted?

For military security purposes it is sufficient that most (not all) of the targets be concealed in real time (not necessarily unlocatable after the fact). Verification is very difficult if we have to maintain a complete tally of the opponent's systems and match them against the permitted limits. We can take a different approach to this by an ordered accounting approach. Each side will be under the obligation of maintaining its own up-to-date location roster of every mobile land-based system. Our task is now to verify the authenticity of that roster: two approaches suggest themselves. Each of them could also be connected with a tagging regime.

1) Ex post facto verification. On this principle each side would be under the obligation to produce, on challenge, a complete location roster as of some stated time, say, three months or six months prior to the date of challenge. If we have intelligence that discovers a single unit out of order, not represented in the roster given as an accounting, we would infer they had cheated. Our challenges would of course be triggered by observations that we believe to be suspicious -- for example of units that we had reason to believe there had been some special effort to conceal.

Since existing operating doctrine embraces deployment at locatable garrisons in peace time, the obligation to exchange retrospective reports should not be burdensome from a security point of view. Conversely, a delay of three months in verification would be a small part of the time required for the political process to react to any but the most flagrant violations, and the latter present a problem for military intelligence regardless of the arms control framework.

2) The second concept would apply a similar principle in real time if this were deemed necessary. If the veil is pierced for a small fraction of the mobile forces, say less than five percent, this is not a significnat impairment of overall security. On the other hand, revelation on challenge could again be used to verify the authenticity of the accounting roster each side is obligated to maintain. At any time, subject to reasonable overall limits, we could challenge the other side to acknowledge whether or not there was a mobile system at a given coordinate (x,y) and then to demonstrate that this system if posted is in fact part of their continued roster. For the latter purpose we would have to have some system of tamper proof repository giving the host either physical security or a decryption method of denying the corpus of the roster, revealing only that which is obliged by the challenge. We could think figuratively of a file containing n envelopes (where n is the number of allowed mobile systems), each envelope containing the current location of a given system. Upon demand when we present an (x,y), they would have to produce the envelope that shows one and only one system present at a specified coordinate. Or else, they would have to deny the presence of a mobile system at (x,y).

If necessary they could be permitted to have a number of additional dummy entries in a given envelope if they were concerned that we might have access to some envelopes we were not entitled to but that is a minor embelishment.

The statistical analysis is very similar to that for tagged systems. If there are, say, two thousand mobile systems access to as few as twenty to fifty envelopes would identify ringers even though they were merely a few percent of the total.

Of course none of the above procedures can help us find a totally concealed unit. But these approaches transform the verification of the total numerical account into the discovery of any unrostered individual unit.

Joshua Lederberg